examundo

Examen de práctica AWS Solutions Architect en español

69 preguntas con respuestas. Las guías y las traducciones las hizo y las revisó un software. Ninguna persona las ha revisado todavía.

Actualizado el 25 de noviembre de 2026 · examundo.tech/es/aws-solutions-architect/

Arquitecturas de alto rendimiento

1. Un clúster HPC con cargas MPI estrechamente acopladas en instancias c5n.18xlarge necesita evitar el kernel del sistema operativo en la comunicación entre nodos para lograr la menor latencia posible a gran escala. ¿Qué función de red se debe asociar a las instancias?

An HPC cluster running tightly coupled MPI workloads across c5n.18xlarge instances needs to bypass the operating system kernel for inter-node communication to achieve the lowest possible latency at scale. Which networking feature should be attached to the instances?

A. Redes mejoradas (enhanced networking) con Elastic Network Adapter (ENA)

B. AWS Global Accelerator con direcciones IP estáticas anycast

C. Una segunda interfaz de red elástica (ENI) para separar el tráfico

D. Elastic Fabric Adapter (EFA)

---

2. Una aplicación hace millones de lecturas por segundo en una tabla de DynamoDB y necesita tiempos de respuesta de microsegundos sin modificar el modelo de datos. ¿Qué solución lo logra MEJOR?

An application performs millions of reads per second against a DynamoDB table and requires microsecond-level response times without modifying the application's data model. Which solution BEST achieves this?

A. DynamoDB Global Tables

B. Amazon DynamoDB Accelerator (DAX)

C. Amazon ElastiCache for Redis delante de DynamoDB

D. DynamoDB Auto Scaling con más RCU aprovisionadas

---

3. Una empresa de medios procesa trabajos cortos de transcodificación de video que duran pocos minutos y llegan en momentos impredecibles durante el día. ¿Qué opción de cómputo es la MÁS económica y exige la MENOR administración de infraestructura?

A media company processes short video transcoding jobs that run for only a few minutes at unpredictable intervals throughout the day. Which compute option is MOST cost-effective and requires the LEAST infrastructure management?

A. Un grupo de Auto Scaling de Amazon EC2 con mínimo una instancia On-Demand

B. Amazon Lightsail con una instancia de tamaño fijo

C. AWS Lambda

D. Instancias EC2 reservadas que funcionan de forma continua

---

4. Una carga de almacén de datos necesita un solo volumen EBS que entregue 200,000 IOPS y 3,000 MB/s de rendimiento (throughput) con latencia constante de menos de un milisegundo, conectado a un tipo de instancia EC2 compatible con io2. ¿Qué tipo de volumen cumple el requisito?

A data warehouse workload requires a single EBS volume delivering 200,000 IOPS and 3,000 MB/s throughput with consistent sub-millisecond latency, attached to an io2-eligible EC2 instance type. Which volume type can meet this requirement?

A. io2 Block Express

B. gp3, aumentando las IOPS y el rendimiento aprovisionados por encima de la base

C. st1 con varios volúmenes en franjas (striping) RAID 0

D. io2 estándar (sin Block Express)

---

5. Usuarios de Asia, Europa y Sudamérica suben archivos multimedia grandes (2 a 10 GB) directamente a un solo bucket de S3 en us-east-1, y los tiempos de carga son irregulares y lentos. ¿Qué solución mejora MEJOR el rendimiento de carga para todas las regiones?

Users across Asia, Europe, and South America upload large media files (2-10 GB) directly to a single S3 bucket located in us-east-1, and upload times are inconsistent and slow. Which solution BEST improves upload performance for all regions?

A. Habilitar solo la carga multiparte (multipart upload), sin otros cambios

B. Habilitar S3 Transfer Acceleration en el bucket

C. Replicar el bucket en cada región con la replicación entre regiones (Cross-Region Replication) de S3

D. Crear una distribución de CloudFront delante del bucket

---

6. Un arquitecto de soluciones debe escalar el tráfico de lectura de una base de datos compatible con MySQL y necesita un retraso de réplica normalmente menor de 100 milisegundos, con hasta 15 réplicas de lectura que compartan el mismo almacenamiento que la instancia principal. ¿Qué solución cumple los requisitos?

A solutions architect must scale read traffic for a MySQL-compatible database and needs replica lag typically under 100 milliseconds, along with support for up to 15 read replicas that share the same underlying storage as the primary instance. Which solution meets these requirements?

A. Amazon Aurora MySQL con réplicas de Aurora

B. Amazon DynamoDB Accelerator (DAX)

C. Amazon RDS for MySQL con réplicas de lectura

D. Una implementación Multi-AZ de Amazon RDS for MySQL

---

7. Un arquitecto de soluciones diseña el almacenamiento de una base de datos relacional crítica en Amazon EC2 que necesita hasta 200,000 IOPS y latencia constante de menos de un milisegundo. ¿Qué tipo de volumen EBS debe elegir?

A solutions architect is designing storage for a mission-critical relational database on Amazon EC2 that requires up to 200,000 IOPS and sub-millisecond, consistent latency. Which EBS volume type should the architect select?

A. SSD de uso general (gp3)

B. HDD en frío (sc1)

C. SSD de IOPS aprovisionadas (io2 Block Express)

D. HDD optimizado para rendimiento (st1)

---

8. Una empresa de medios global quiere reducir la latencia de los usuarios que ven video en streaming guardando copias del contenido en ubicaciones físicamente más cercanas a ellos. ¿Qué servicio de AWS debe usar?

A global media company wants to reduce latency for users streaming video content by caching copies of the content at locations physically closer to end users. Which AWS service should be used?

A. Amazon ElastiCache
B. AWS Direct Connect
C. Amazon Route 53
D. Amazon CloudFront

---

9. Un sitio de comercio electrónico global usa CloudFront con ubicaciones de borde en varios continentes, y el servidor de origen tiene mucha carga por fallos repetidos de caché (cache misses) de los mismos objetos entre las cachés regionales de borde. ¿Qué función de CloudFront debe habilitar el arquitecto para reducir la carga del origen?

A global e-commerce site uses CloudFront with edge locations on multiple continents, and the origin server is experiencing high load from repeated cache misses across regional edge caches for the same objects. Which CloudFront feature should the solutions architect enable to reduce origin load?

A. URL firmadas (signed URLs)
B. Cifrado a nivel de campo (field-level encryption)
C. Disparadores de solicitud de origen de Lambda@Edge
D. Origin Shield

---

10. Un sitio web global servido con Amazon CloudFront genera mucha carga en sus servidores de origen porque muchas ubicaciones de borde obtienen por separado los mismos objetos, que rara vez están en caché, cuando hay fallos de caché (cache misses). ¿Qué función reduce MEJOR esa carga sin cambiar la estrategia de TTL de la caché?

A global website served through Amazon CloudFront experiences high load on its origin servers because many edge locations independently fetch the same rarely-cached objects from the origin during cache misses. Which feature BEST reduces this origin load without changing the caching TTL strategy?

A. Aumentar el TTL de caché de todos los objetos
B. Aumentar la capacidad de cómputo del servidor de origen
C. Habilitar CloudFront Origin Shield
D. Implementar Lambda@Edge para servir contenido estático

---

11. Una aplicación escribe en un bucket de Amazon S3 a un ritmo sostenido de 12,000 solicitudes PUT por segundo, y todas las claves de objeto empiezan con el mismo prefijo. El rendimiento de carga está bajando. ¿Cuál es la solución MÁS eficaz?

An application writes to an Amazon S3 bucket at a sustained rate of 12,000 PUT requests per second, with all object keys beginning with the same prefix. Upload performance is degrading. What is the MOST effective solution?

A. Habilitar el control de versiones de S3 en el bucket
B. Cambiar la clase de almacenamiento a S3 Standard-IA
C. Distribuir los objetos en varios prefijos de clave
D. Habilitar S3 Transfer Acceleration en el bucket

---

12. Una aplicación en clúster que se ejecuta en varias instancias EC2 de la misma zona de disponibilidad necesita almacenamiento en bloques compartido y de baja latencia, con acceso simultáneo de lectura y escritura desde hasta 16 instancias. ¿Qué solución cumple el requisito?

A clustered application running on multiple EC2 instances in the same Availability Zone requires shared, low-latency block storage with concurrent read/write access from up to 16 instances. Which solution meets this requirement?

A. Amazon S3 con Transfer Acceleration
B. Amazon EBS io2 con Multi-Attach
C. Amazon EFS
D. Amazon EBS gp3 con instantáneas (snapshots)

---

13. Una aplicación HPC estrechamente acoplada necesita la menor latencia de red posible y el mayor rendimiento (throughput) entre instancias EC2 dentro de una sola zona de disponibilidad. ¿Qué estrategia de ubicación de EC2 debe usar el arquitecto?

A tightly coupled HPC application requires the lowest possible network latency and highest throughput between EC2 instances within a single Availability Zone. Which EC2 placement strategy should the architect use?

A. Grupo de ubicación en clúster (cluster placement group)
B. Grupo de ubicación disperso (spread placement group)
C. Ubicación predeterminada (sin grupo)
D. Grupo de ubicación por particiones (partition placement group)

---

14. Un arquitecto de soluciones quiere reducir la carga de lectura de una base de datos relacional guardando en memoria los resultados de consultas de uso frecuente. ¿Qué servicio de AWS está diseñado para esto?

A solutions architect wants to reduce read load on a relational database by caching frequently accessed query results in memory. Which AWS service is designed for this purpose?

A. Amazon DynamoDB Accelerator (DAX)
B. AWS Storage Gateway
C. Amazon ElastiCache
D. Amazon CloudFront

---

15. Una empresa de videojuegos necesita una caché simple en memoria para guardar datos de sesión y quiere aprovechar el procesamiento multihilo para lograr el máximo rendimiento en un solo nodo de caché grande. ¿Qué motor de caché debe elegir el arquitecto de soluciones?

A gaming company needs a simple in-memory cache to store session data and wants to take advantage of multi-threaded processing to maximize throughput on a single large cache node. Which caching engine should the solutions architect select?

A. Amazon ElastiCache for Redis
B. Amazon DynamoDB Accelerator (DAX)
C. Amazon ElastiCache for Memcached
D. Amazon RDS Proxy

---

16. Una empresa de videojuegos usa una caché de estado de sesión en ElastiCache y quiere maximizar el rendimiento por nodo aprovechando todos los núcleos de CPU de la instancia. Los datos no requieren persistencia, replicación ni estructuras de datos complejas. ¿Qué motor de ElastiCache cumple MEJOR el requisito?

A gaming company runs an ElastiCache session-state cache and wants to maximize throughput per node by fully utilizing all CPU cores on the underlying instance. The data does not require persistence, replication, or complex data structures. Which ElastiCache engine BEST meets this requirement?

A. Memcached
B. Redis con el modo de clúster deshabilitado
C. Redis con el modo de clúster habilitado
D. Redis con Multi-AZ y conmutación por error automática

---

17. Una empresa aloja recursos estáticos de un sitio web en un bucket de S3 en us-east-1 y atiende a usuarios de Norteamérica, Europa y Asia. Los usuarios de Asia reportan que las páginas cargan lento. ¿Qué solución da la MAYOR mejora de rendimiento con la MENOR carga operativa?

A company hosts static website assets in an S3 bucket in us-east-1 and serves users across North America, Europe, and Asia. Users in Asia report slow page load times. Which solution provides the MOST performance improvement with the LEAST operational overhead?

A. Implementar una distribución de Amazon CloudFront con el bucket de S3 como origen

B. Crear replicación entre regiones de S3 hacia buckets en cada región

C. Aumentar el tamaño de la instancia EC2 que aloja el servidor web

D. Habilitar S3 Transfer Acceleration en el bucket

Arquitecturas seguras

18. Una organización quiere que los desarrolladores creen roles y políticas de IAM para sus propios proyectos, pero debe garantizar que ninguno pueda dar a un rol permisos más amplios que un máximo predefinido, sin importar la política que adjunte. ¿Qué función de IAM debe implementar el arquitecto de soluciones?

An organization wants to allow developers to create IAM roles and policies for their own projects, but must guarantee that no developer can grant a role permissions broader than a predefined maximum, regardless of the policy they attach. Which IAM feature should the solutions architect implement?

A. Una política de grupo de IAM más restrictiva que cualquier política que los desarrolladores puedan adjuntar

B. Una política de control de servicios (SCP) adjunta a la unidad organizativa de los desarrolladores

C. Un límite de permisos adjunto a cada rol de IAM que creen los desarrolladores

D. Una política basada en recursos en cada recurso al que accederán los roles

19. Un arquitecto de soluciones diseña una aplicación en instancias EC2 que necesita leer objetos de un bucket de S3. ¿Qué enfoque es el MÁS seguro para dar ese acceso?

A solutions architect is designing an application running on EC2 instances that needs to read objects from an S3 bucket. Which approach provides the MOST secure method for granting this access?

A. Incluir las credenciales del usuario raíz de la cuenta de AWS en el archivo de configuración de la aplicación

B. Crear un usuario de IAM con acceso a S3 y escribir sus credenciales en el código de la aplicación

C. Asociar al perfil de instancia de EC2 un rol de IAM con una política que conceda s3:GetObject

D. Guardar las claves de acceso de un usuario de IAM en las variables de entorno de la instancia EC2

20. Una empresa de comercio electrónico en AWS quiere contacto proactivo del equipo de respuesta a DDoS de AWS (DRT, hoy Shield Response Team) y protección de costos ante los cargos por escalado durante un ataque DDoS de gran escala. ¿Qué nivel de servicio debe habilitar el arquitecto?

An e-commerce company running on AWS wants proactive engagement from the AWS DDoS Response Team (DRT) and cost protection against scaling charges incurred during a large-scale DDoS attack. Which service tier should the architect enable?

A. Amazon GuardDuty con protección para S3 habilitada

B. AWS Shield Standard, que se incluye automáticamente para todos los clientes

C. AWS Shield Advanced

D. AWS WAF solo con reglas basadas en tasa

21. Un arquitecto de soluciones debe asegurar que los datos de los volúmenes de Amazon EBS conectados a instancias EC2 estén cifrados en reposo, incluidas todas las instantáneas creadas a partir de esos volúmenes, con la mínima carga operativa. ¿Qué enfoque debe seguir?

A solutions architect must ensure that data stored on Amazon EBS volumes attached to EC2 instances is encrypted at rest, including all snapshots created from those volumes, with minimal operational overhead. Which approach should the architect take?

A. Habilitar el cifrado predeterminado de S3 en el bucket donde se guardan las instantáneas

B. Aplicar una política de IAM que niegue crear volúmenes sin cifrar, sin habilitar el cifrado a nivel de cuenta

C. Cifrar manualmente cada instantánea después de crearla con una utilidad de cifrado de discos de terceros

D. Habilitar el cifrado de EBS predeterminado en la cuenta y la región, para que los volúmenes nuevos y sus instantáneas se cifren solos con AWS KMS

---

22. Una empresa de servicios financieros guarda documentos confidenciales en Amazon S3 y debe poder auditar cada uso de la clave de cifrado, incluido qué entidad principal descifró un objeto y cuándo. ¿Qué opción de cifrado cumple este requisito?

A financial services company stores sensitive documents in Amazon S3 and must be able to audit every use of the encryption key, including which principal decrypted a given object and when. Which encryption option satisfies this requirement?

A. Cifrado del lado del cliente con una clave guardada localmente

B. SSE-C con una clave enviada en cada solicitud

C. SSE-S3 con claves administradas por Amazon S3

D. SSE-KMS con una clave de KMS administrada por el cliente

---

23. Una empresa conecta su centro de datos local con una VPC mediante AWS Direct Connect. Los servidores locales deben llegar de forma privada a los buckets de Amazon S3, sin pasar por la internet pública y sin usar una puerta de enlace NAT ni un proxy. ¿Qué solución cumple el requisito?

A company connects its on-premises data center to a VPC using AWS Direct Connect. On-premises servers must reach Amazon S3 buckets privately, without traversing the public internet and without using a NAT gateway or proxy. Which solution meets this requirement?

A. Habilitar S3 Transfer Acceleration en los buckets de destino

B. Conectar una puerta de enlace de internet a la VPC y restringir el acceso con una condición de política del bucket sobre la VIF de Direct Connect

C. Crear un punto de enlace de VPC de tipo puerta de enlace (gateway endpoint) para S3 y actualizar las tablas de enrutamiento de la VPC

D. Crear un punto de enlace de VPC de tipo interfaz (interface endpoint) para S3 y actualizar el DNS local para que resuelva a sus IP privadas

---

24. Una política de bucket restringe el acceso con una condición aws:SourceIp limitada al bloque CIDR privado de una VPC corporativa, 10.20.0.0/16. Las instancias EC2 de esa VPC acceden a S3 por la ruta de internet pública a través de una puerta de enlace NAT. Las solicitudes se niegan de forma inesperada. ¿Cuál es la causa raíz?

A bucket policy restricts access using a condition on aws:SourceIp limited to a corporate VPC's private CIDR block, 10.20.0.0/16. EC2 instances in that VPC access S3 over the public internet path through a NAT gateway. Requests are unexpectedly denied. What is the root cause?

A. El bloque CIDR privado debe agregarse a la configuración CORS del bucket

B. La puerta de enlace NAT reemplaza la IP de origen por su propia IP elástica pública, que queda fuera del CIDR permitido

C. Las políticas de bucket de S3 no pueden evaluar aws:SourceIp en ningún tráfico que se origine en una VPC

D. aws:SourceIp solo evalúa direcciones IPv6 cuando las instancias usan una puerta de enlace NAT

---

25. ¿Qué servicio de AWS está diseñado específicamente para dar protección administrada contra ataques de denegación de servicio distribuido (DDoS)?

Which AWS service is purpose-built to provide managed protection against Distributed Denial of Service (DDoS) attacks?

A. AWS Firewall Manager

B. AWS WAF

C. Amazon GuardDuty

D. AWS Shield

---

26. Una empresa debe cifrar objetos en Amazon S3 y mantener un registro de auditoría detallado de cada uso de la clave de cifrado, incluido quién la usó y cuándo. ¿Qué opción de cifrado cumple el requisito?

A company must encrypt objects in Amazon S3 and maintain a detailed audit trail of every use of the encryption key, including who accessed it and when. Which encryption option meets this requirement?

A. Cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3)

B. Cifrado del lado del cliente con una clave AES-256 generada localmente y guardada en el código de la aplicación

C. Cifrado del lado del servidor con claves de AWS KMS (SSE-KMS), usando AWS CloudTrail para registrar el uso de la clave

D. Cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C), enviadas en cada solicitud

---

27. Un arquitecto de soluciones necesita crear, administrar y controlar de forma central el acceso a las claves criptográficas que cifran los objetos guardados en Amazon S3. ¿Qué servicio de AWS debe usar?

A solutions architect needs to centrally create, manage, and control access to the cryptographic keys used to encrypt objects stored in Amazon S3. Which AWS service should be used?

A. AWS Systems Manager Parameter Store

B. AWS Secrets Manager

C. AWS Key Management Service (KMS)

D. AWS Certificate Manager (ACM)

---

28. Un arquitecto de soluciones escribe una política de IAM para un grupo de desarrolladores que deben poder leer y escribir objetos solo dentro del prefijo 'dev-uploads' de un único bucket de S3, y no deben acceder a ningún otro bucket de la cuenta. ¿Qué diseño de política sigue el principio de mínimo privilegio?

A solutions architect is writing an IAM policy for a group of developers who must be able to read and write objects only within the 'dev-uploads' prefix of a single S3 bucket, and must not access any other bucket in the account. Which policy design follows the principle of least privilege?

A. Conceder s3:GetObject y s3:PutObject en el Resource "*" y confiar en la política del bucket para restringir el acceso

B. Adjuntar la política administrada AmazonS3FullAccess y confiar en la disciplina de los desarrolladores

C. Conceder las acciones s3:* con un elemento Resource limitado a arn:aws:s3:::company-bucket/dev-uploads/*

D. Conceder s3:GetObject y s3:PutObject con un elemento Resource limitado a arn:aws:s3:::company-bucket/dev-uploads/*

---

29. Un usuario tiene una política de IAM basada en identidad que permite s3:GetObject en todos los recursos. El usuario también es miembro de un grupo cuya política niega de forma explícita s3:GetObject en un bucket específico. Cuando el usuario intenta obtener un objeto de ese bucket, ¿cuál es el resultado?

A user has an IAM identity-based policy that allows s3:GetObject on all resources. The user is also a member of a group whose policy explicitly denies s3:GetObject on a specific bucket. When the user attempts to retrieve an object from that bucket, what is the result?

A. Se permite el acceso porque la política de permiso del usuario tiene prioridad sobre las políticas de grupo

B. Se niega el acceso porque una denegación explícita en cualquier política aplicable siempre anula un permiso

C. Se permite el acceso porque IAM evalúa solo la política adjuntada más recientemente

D. Se niega el acceso solo si la denegación está adjunta directamente al usuario y no a un grupo

---

30. Un rol de IAM de la cuenta B (333333333333) tiene una política basada en identidad que concede kms:Decrypt con Resource "*". El rol intenta descifrar un objeto de S3 cifrado con una clave de KMS administrada por el cliente que pertenece a la cuenta A (222222222222) y recibe un error AccessDenied. ¿Cuál es la causa MÁS probable?

An IAM role in Account B (333333333333) has an identity-based policy granting kms:Decrypt with Resource set to "*". The role attempts to decrypt an S3 object encrypted with a customer-managed KMS key owned by Account A (222222222222) and receives an AccessDenied error. What is the MOST likely cause?

A. La política de clave de la CMK en la cuenta A no incluye una instrucción que conceda kms:Decrypt a entidades principales de la cuenta B

B. El elemento Resource de la política de IAM debe indicar el ARN específico de la clave y no un comodín en llamadas entre cuentas

C. La política del bucket de S3 en la cuenta A debe permitir por separado la acción kms:Decrypt a la cuenta B

D. El rol necesita una concesión (grant) de KMS en lugar de una política de IAM basada en identidad para descifrar

---

31. Un arquitecto de soluciones explica cómo AWS KMS cifra objetos grandes de forma eficiente. ¿Qué afirmación describe MEJOR el proceso de cifrado de sobre (envelope encryption) que usa KMS?

A solutions architect is explaining how AWS KMS encrypts large objects efficiently. Which statement BEST describes the envelope encryption process used by KMS?

A. KMS guarda el objeto en texto plano directamente dentro de la clave maestra del cliente

B. KMS cifra el objeto completo directamente con la clave maestra del cliente, sin ninguna clave intermedia

C. KMS exige que la aplicación genere y administre a mano su propia clave AES sin llamar a la API de KMS

D. KMS genera una clave de datos, que se usa para cifrar el objeto localmente, y la clave de datos cifrada se guarda junto con el texto cifrado

---

32. Un equipo guarda la contraseña de una base de datos de Amazon RDS y quiere que se rote automáticamente cada 30 días con una función de rotación de Lambda incluida, sin escribir lógica de rotación propia. ¿Qué servicio cumple MEJOR este requisito?

A team stores an Amazon RDS database password and wants it automatically rotated every 30 days using a built-in Lambda rotation function, without writing custom rotation logic. Which service BEST satisfies this requirement?

A. AWS KMS con la rotación anual automática de claves habilitada

B. AWS Systems Manager Parameter Store con parámetros SecureString

C. AWS Secrets Manager con la compatibilidad nativa de rotación para RDS

D. Tokens de autenticación de base de datos de IAM

---

33. Durante una investigación de seguridad, un arquitecto necesita saber qué direcciones IP de origen enviaron tráfico a la interfaz de red elástica de una instancia EC2 específica y si el grupo de seguridad aceptó o rechazó ese tráfico. ¿Qué servicio de AWS da esta información?

During a security investigation, an architect needs to determine which source IP addresses sent traffic to a specific EC2 instance's elastic network interface and whether that traffic was accepted or rejected by the security group. Which AWS service provides this information?

A. AWS CloudTrail

B. VPC Flow Logs

C. Amazon Inspector

D. AWS Config

---

34. Un equipo de aplicaciones debe restringir el tráfico saliente de una subred de aplicación para que las instancias solo lleguen a una lista aprobada de nombres de dominio externos (por ejemplo, api.partner.com), sin importar la dirección IP de destino, que cambia con frecuencia. ¿Qué control cumple este requisito?

An application team must restrict outbound traffic from an application subnet so instances can only reach a specific approved list of external domain names (e.g., api.partner.com), regardless of the destination IP address, which changes frequently. Which control enforces this requirement?

A. AWS Network Firewall con un grupo de reglas con estado basado en dominios que permita los FQDN aprobados

B. Una regla saliente de ACL de red que permita HTTPS a las IP actuales de los dominios aprobados

C. Una política de punto de enlace de puerta de enlace de S3 limitada a los dominios aprobados del socio

D. Una regla saliente de grupo de seguridad que enumere los rangos CIDR de destino de los dominios aprobados

---

35. Un administrador de bases de datos descubre que una instancia de producción de RDS for MySQL se lanzó sin cifrado en reposo. Ahora el cumplimiento normativo exige cifrar todos los datos en reposo con una clave de KMS administrada por el cliente, con el mínimo tiempo de inactividad. ¿Cuál es la secuencia de acciones correcta?

A database administrator discovers that an existing production RDS for MySQL instance was launched without encryption at rest enabled. Compliance now requires all data at rest to be encrypted using a customer managed KMS key, with minimal downtime. What is the correct sequence of actions?

A. Crear una réplica de lectura con cifrado habilitado y promoverla para reemplazar la instancia principal

B. Tomar una instantánea de la instancia sin cifrar, copiarla con el cifrado habilitado y restaurar una instancia nueva desde la copia cifrada

C. Modificar la instancia de RDS existente, habilitar la opción "Encryption at rest" y reiniciarla para aplicar el cambio

D. Habilitar el cifrado directamente en la instancia en ejecución con el comando modify-db-instance de la AWS CLI

Arquitecturas optimizadas en costos

36. Un arquitecto de soluciones necesita ejecutar un trabajo por lotes tolerante a fallos que puede interrumpirse en cualquier momento, a cambio del mayor descuento posible sobre el precio On-Demand. ¿Qué opción de compra de EC2 es la MÁS adecuada?

A solutions architect needs to run a fault-tolerant batch processing job that can be interrupted at any time in exchange for the deepest possible discount off On-Demand pricing. Which EC2 purchasing option is MOST appropriate?

A. Instancias reservadas estándar (Standard Reserved Instances)

B. Instancias Spot

C. Instancias On-Demand

D. Hosts dedicados (Dedicated Hosts)

---

37. Una empresa ejecuta una carga de base de datos de forma continua, las 24 horas, durante los próximos tres años y quiere minimizar el costo de cómputo con un compromiso firme de capacidad. ¿Qué opción de compra da el mayor descuento para esta carga estable?

A company runs a database workload continuously, 24 hours a day, for the next three years and wants to minimize compute cost with a firm capacity commitment. Which purchasing option provides the largest discount for this steady-state workload?

A. Instancias reservadas estándar con plazo de 3 años

B. Instancias reservadas convertibles con plazo de 1 año

C. Instancias Spot

D. Instancias On-Demand

---

38. Una empresa sirve archivos de video grandes directamente desde Amazon S3 a usuarios de todo el mundo y paga altos cargos por transferencia de datos de salida (OUT). ¿Qué cambio reduce MÁS estos costos y además mejora el rendimiento?

A company serves large video files directly from Amazon S3 to users worldwide, incurring high data transfer OUT charges. Which change MOST reduces these costs while also improving performance?

A. Implementar Amazon CloudFront delante del bucket de S3 con un Origin Access Control

B. Habilitar S3 Transfer Acceleration en el bucket

C. Mover los archivos de video a S3 One Zone-Infrequent Access

D. Replicar el bucket en todas las regiones de AWS con la replicación entre regiones (Cross-Region Replication)

---

39. Una base de datos de producción necesita 16,000 IOPS sostenidas y 500 MB/s de rendimiento (throughput) en un volumen de 500 GB. ¿Qué tipo de volumen EBS cumple el requisito al MENOR costo?

A production database requires a sustained 16,000 IOPS and 500 MB/s throughput on a 500 GB volume. Which EBS volume type meets this requirement at the LOWEST cost?

A. io1
B. gp2
C. gp3
D. io2

---

40. Una empresa determinó que su carga de producción se ejecutará en la misma familia de instancias EC2, el mismo tamaño, la misma región y el mismo sistema operativo durante los próximos 3 años, sin cambios previstos. ¿Qué opción de compra da el MAYOR descuento sobre el precio On-Demand?

A company has determined that its production workload will run on the same EC2 instance family, size, Region, and operating system for the next 3 years with no anticipated changes. Which purchasing option provides the HIGHEST discount off On-Demand pricing?

A. Compute Savings Plans (plazo de 3 años)
B. Instancias reservadas estándar (plazo de 1 año, sin pago inicial)
C. Instancias reservadas convertibles (plazo de 3 años, pago total por adelantado)
D. Instancias reservadas estándar (plazo de 3 años, pago total por adelantado)

---

41. Una empresa compra instancias reservadas para una carga de producción, pero prevé migrar en los próximos 18 meses a tipos de instancia nuevos y más eficientes, lo que podría cambiar la familia de instancias y el sistema operativo. ¿Qué tipo de instancia reservada debe elegir?

A company purchases Reserved Instances for a production workload but anticipates migrating to newer, more cost-efficient instance types within the next 18 months as they become available, potentially changing instance family and operating system. Which Reserved Instance type should be selected?

A. Instancias reservadas convertibles
B. Instancias reservadas estándar
C. Instancias reservadas programadas (Scheduled Reserved Instances)
D. Instancias reservadas zonales

---

42. Un arquitecto de soluciones quiere reducir los costos de almacenamiento EBS de una carga de uso general y a la vez garantizar una base de 3,000 IOPS y 125 MiB/s de rendimiento (throughput) sin importar el tamaño del volumen. ¿Qué tipo de volumen debe elegir?

A solutions architect wants to reduce EBS storage costs for a general-purpose workload while still guaranteeing a baseline of 3,000 IOPS and 125 MiB/s throughput regardless of volume size. Which volume type should be selected?

A. gp3
B. gp2
C. io2 Block Express
D. st1

---

43. Una empresa de medios ejecuta cada noche un trabajo por lotes de transcodificación de video que guarda su progreso (checkpoint) y puede reanudarse si se interrumpe. Minimizar el costo de cómputo es la prioridad principal. ¿Qué opción de compra de EC2 es la MÁS económica?

A media company runs a nightly video transcoding batch job that checkpoints progress and can resume if interrupted. Minimizing compute cost is the top priority for this workload. Which EC2 purchasing option is MOST cost-effective?

A. Hosts dedicados
B. Instancias reservadas
C. Instancias On-Demand
D. Instancias Spot

---

44. Una empresa ejecuta una base de datos PostgreSQL de producción en Amazon RDS con uso continuo, estable y predecible en el futuro cercano. ¿Qué opción de compra MINIMIZA el costo de esta base de datos?

A company runs a production PostgreSQL database on Amazon RDS that operates continuously with predictable, steady-state usage for the foreseeable future. Which purchasing option MINIMIZES cost for this database?

A. Instancias Spot para RDS
B. Instancias de base de datos On-Demand
C. RDS Serverless v2 aprovisionado con el máximo de ACU
D. Instancias reservadas de RDS

---

45. Una empresa debe conservar registros de cumplimiento durante 10 años. Se consultan más o menos una vez al año y, cuando se consultan, los resultados deben estar disponibles en minutos y no en horas. ¿Qué clase de almacenamiento de S3 tiene el MENOR costo y cumple el requisito de recuperación?

A company must retain compliance records for 10 years. The records are accessed roughly once per year, and when accessed, results must be available within minutes rather than hours. Which S3 storage class provides the LOWEST cost while meeting the retrieval requirement?

A. S3 Standard-IA
B. S3 Glacier Flexible Retrieval
C. S3 One Zone-IA
D. S3 Glacier Deep Archive

---

46. Una empresa aloja en Amazon S3 un conjunto de datos de investigación público que investigadores externos de todo el mundo descargan con frecuencia. La empresa quiere que los usuarios externos paguen la transferencia de datos de las descargas y los costos de solicitudes, y no el propietario del bucket. ¿Qué función de S3 debe habilitar?

A company hosts a publicly available research dataset in Amazon S3 that is downloaded frequently by external researchers around the world. The company wants external users to pay for the download data transfer and request costs instead of the bucket owner. Which S3 feature should be enabled?

A. Replicación en la misma región de S3 (Same-Region Replication)
B. S3 Requester Pays
C. S3 Object Lock
D. S3 Transfer Acceleration

---

47. Una empresa de medios guarda millones de objetos con patrones de acceso impredecibles y cambiantes: algunos se consultan con frecuencia, otros no se tocan durante meses, y es imposible saber cuáles. ¿Qué estrategia de almacenamiento de S3 minimiza el costo con la MENOR carga operativa?

A media company stores millions of objects with unpredictable, changing access patterns—some objects are accessed frequently, others go untouched for months, and it is impossible to predict which. Which S3 storage strategy minimizes cost with the LEAST operational overhead?

A. S3 Standard con una regla de ciclo de vida que pase los objetos a S3 Glacier Flexible Retrieval después de 90 días
B. S3 Intelligent-Tiering
C. S3 One Zone-IA para todos los objetos
D. S3 Standard con una regla de ciclo de vida que pase los objetos a S3 Standard-IA después de 30 días

---

48. ¿Qué opción de pago de instancias reservadas da el MAYOR descuento frente al precio On-Demand para el mismo plazo?

Which Reserved Instance payment option provides the LARGEST discount compared to On-Demand pricing for the same term length?

A. Sin pago inicial (No Upfront)
B. Pago total por adelantado (All Upfront)
C. Pagos mensuales sin compromiso
D. Pago inicial parcial (Partial Upfront)

---

49. ¿Qué modelo de precios de EC2 no requiere pago inicial ni compromiso a largo plazo y factura por segundo en instancias Linux, lo que lo hace ideal para cargas de corta duración e impredecibles?

Which EC2 pricing model requires no upfront payment or long-term commitment and bills by the second for Linux instances, making it best suited for short-term, unpredictable workloads?

A. Instancias On-Demand
B. Instancias Spot
C. Instancias reservadas
D. Savings Plans

---

50. Una arquitectura replica cada noche datos de un bucket de S3 en us-east-1 a un bucket en eu-west-1, para recuperación ante desastres, con la replicación entre regiones (Cross-Region Replication) de S3. ¿Qué costo debe considerar el arquitecto de soluciones que NO se aplicaría con la replicación en la misma región (Same-Region Replication)?

An architecture replicates data nightly from an S3 bucket in us-east-1 to a bucket in eu-west-1 for disaster recovery using S3 Cross-Region Replication. Which cost should the solutions architect account for that would NOT apply with Same-Region Replication?

A. Cargos de transferencia de datos entre regiones
B. Cargos de solicitudes PUT de S3
C. Cargos de almacenamiento de S3 en el bucket de destino
D. Cargos de S3 Replication Time Control

---

51. Un arquitecto de soluciones quiere una solución de almacenamiento de S3 que mueva automáticamente los objetos entre niveles de acceso frecuente y poco frecuente según los cambios en los patrones de acceso, sin afectar el rendimiento y sin reglas de ciclo de vida manuales. ¿Qué clase de almacenamiento debe usar?

A solutions architect wants an S3 storage solution that automatically moves objects between frequent and infrequent access tiers based on changing access patterns, without performance impact or manual lifecycle rules. Which storage class should be used?

A. S3 One Zone-IA
B. S3 Standard-IA
C. S3 Glacier Instant Retrieval
D. S3 Intelligent-Tiering

---

52. Una startup tiene una VPC de desarrollo con poco tráfico, cuyas instancias en subredes privadas necesitan acceso saliente a internet, y quiere minimizar el costo mensual. ¿Cuál es la forma MENOS costosa de dar esta conectividad?

A startup runs a low-traffic development VPC that needs outbound internet access for private subnet instances and wants to minimize monthly cost. Which option is the LEAST expensive way to provide this connectivity?

A. Dos puertas de enlace NAT (NAT Gateways) para alta disponibilidad
B. AWS Direct Connect
C. Una sola instancia NAT (NAT instance) en un tipo de instancia EC2 pequeño
D. Una puerta de enlace NAT en cada zona de disponibilidad

Arquitecturas resilientes

53. Una empresa minorista quiere crear una arquitectura basada en eventos en la que las actualizaciones de inventario de varios sistemas internos activen acciones independientes en varios microservicios, con la posibilidad de filtrar los eventos por contenido antes de enrutarlos. ¿Qué servicio de AWS es la MEJOR opción para el bus de eventos?

A retail company wants to build an event-driven architecture where inventory updates from multiple internal systems trigger independent actions in several downstream microservices, with the ability to filter events by content before routing. Which AWS service is the BEST fit for the event bus?

A. Amazon SQS
B. Amazon EventBridge
C. AWS Step Functions
D. Amazon Kinesis Data Streams

---

54. Una empresa de videojuegos ejecuta una aplicación multijugador basada en TCP y sensible a la latencia en varias regiones de AWS, y necesita dirigir a los jugadores al punto de conexión más saludable y de menor latencia, con direcciones IP estáticas anycast. ¿Qué servicio debe usar el arquitecto de soluciones?

A gaming company runs a latency-sensitive TCP-based multiplayer application across multiple AWS Regions and needs to route players to the healthiest, lowest-latency endpoint while providing static anycast IP addresses. Which service should the solutions architect use?

A. Enrutamiento basado en latencia de Amazon Route 53
B. AWS Global Accelerator
C. Balanceo de carga entre zonas (cross-zone) de Elastic Load Balancing
D. Amazon CloudFront

---

55. Una base de datos de producción de Amazon RDS for MySQL está implementada con Multi-AZ. El host subyacente de la zona de disponibilidad principal sufre una falla de hardware. ¿Qué ocurre desde el punto de vista de la aplicación durante la conmutación por error automática?

A production Amazon RDS for MySQL database is deployed in a Multi-AZ configuration. The underlying host in the primary Availability Zone experiences a hardware failure. What occurs from the application's perspective during the automatic failover?

A. El punto de conexión de la instancia de base de datos (CNAME) se actualiza para resolver a la instancia en espera, y la aplicación se reconecta sin cambiar la cadena de conexión
B. El administrador de la base de datos debe actualizar a mano la cadena de conexión de la aplicación para apuntar a la instancia en espera
C. La réplica de lectura más cercana de la misma región se promueve automáticamente a nueva instancia principal
D. Las comprobaciones de estado de Amazon Route 53 detectan la falla y redirigen el tráfico a la instancia en espera

---

56. Un arquitecto de soluciones debe diseñar una base de datos multirregión activo-activo para una aplicación global que requiere lecturas y escrituras de baja latencia en cada región, con resolución automática de conflictos. ¿Qué solución cumple el requisito?

A solutions architect must design a multi-region active-active database for a global application that requires low-latency reads and writes in each Region with automatic conflict resolution. Which solution meets this requirement?

A. Amazon ElastiCache for Redis con el modo de clúster habilitado
B. Tablas globales de Amazon DynamoDB
C. Una implementación Multi-AZ de Amazon RDS
D. Réplicas de lectura de Amazon RDS en cada región

---

57. La aplicación interna de informes de una startup tolera hasta 24 horas de inactividad y hasta 24 horas de pérdida de datos si ocurre un desastre regional. Minimizar el costo es la prioridad principal del diseño de recuperación ante desastres. ¿Qué estrategia es la MÁS adecuada?

A startup's internal reporting application can tolerate up to 24 hours of downtime and up to 24 hours of data loss in the event of a regional disaster. Cost minimization is the top priority for the disaster recovery design. Which strategy is MOST appropriate?

A. Luz piloto (pilot light)
B. Multisitio activo-activo (multi-site active-active)
C. Espera semiactiva (warm standby)
D. Copia de seguridad y restauración (backup and restore)

---

58. La estrategia de recuperación ante desastres de una empresa mantiene siempre en una región secundaria una copia reducida pero totalmente funcional de su entorno de producción. Durante una caída regional, la empresa escala el entorno secundario para atender todo el tráfico de producción. ¿Qué estrategia de recuperación es esta?

A company's disaster recovery strategy runs a scaled-down but fully functional copy of its production environment in a secondary region at all times. During a regional outage, the company scales up the secondary environment to handle full production traffic. Which DR strategy is this?

A. Multisitio activo-activo (multi-site active-active)
B. Espera semiactiva (warm standby)
C. Luz piloto (pilot light)
D. Copia de seguridad y restauración (backup and restore)

---

59. Un arquitecto de soluciones diseña una aplicación web de tres capas que debe seguir disponible si una zona de disponibilidad completa deja de estar disponible. ¿Qué opción de arquitectura para la capa de base de datos cumple MEJOR este requisito?

A solutions architect is designing a three-tier web application that must remain available if an entire Availability Zone becomes unavailable. Which architecture choice for the database tier BEST meets this requirement?

A. Una sola instancia de Amazon RDS con instantáneas diarias automáticas
B. Una implementación Multi-AZ de Amazon RDS con una instancia en espera síncrona en una segunda zona de disponibilidad
C. Amazon RDS con una réplica de lectura en la misma zona de disponibilidad que la instancia principal
D. Una implementación de Amazon RDS en una sola zona detrás de un Elastic Load Balancer

---

60. Un arquitecto de soluciones diseña una aplicación multirregión activo-activo con tablas globales de Amazon DynamoDB. Dos usuarios de regiones distintas actualizan el mismo elemento al mismo tiempo, antes de que termine la replicación. ¿Qué afirmación describe correctamente cómo resuelven este conflicto las tablas globales de DynamoDB?

A solutions architect is designing an active-active multi-region application using Amazon DynamoDB Global Tables. Two users in different regions update the same item simultaneously before replication completes. Which statement correctly describes how DynamoDB Global Tables resolves this conflict?

A. DynamoDB aplica la política de que gana la última escritura, según la marca de tiempo de cada una, y la más reciente se propaga a todas las tablas réplica
B. DynamoDB combina los valores de atributos en conflicto en un solo elemento mediante relojes vectoriales
C. DynamoDB rechaza ambas escrituras y devuelve una excepción ConditionalCheckFailedException a los dos clientes
D. DynamoDB pone en cola las escrituras en conflicto y exige que la aplicación las resuelva a mano con una función Lambda antes de seguir replicando

---

61. Los requisitos de recuperación ante desastres de una empresa piden un RTO de 10 minutos y un RPO de 5 minutos para una aplicación crítica de procesamiento de pedidos, con una restricción de costos que impide ejecutar de forma continua la capacidad completa de producción en una segunda región. ¿Qué estrategia cumple MEJOR estos requisitos?

A company's disaster recovery requirements specify an RTO of 10 minutes and an RPO of 5 minutes for a critical order-processing application, with a cost constraint that rules out running full production capacity continuously in a second region. Which DR strategy BEST satisfies these requirements?

A. Pilot light: mantener activa solo la replicación de la base de datos central y crear la capacidad de cómputo desde cero durante un desastre

B. Warm standby: ejecutar en la segunda región una copia reducida pero totalmente funcional de la carga, que se pueda escalar rápido

C. Backup and restore: copiar instantáneas a una segunda región cada 6 horas con AWS Backup

D. Multisitio activo-activo: ejecutar a la vez y siempre la capacidad de producción completa en ambas regiones

---

62. Una empresa de videojuegos necesita una base de datos NoSQL que replique los datos automáticamente entre varias regiones de AWS con escrituras multiactivas, para que los jugadores de cualquier región tengan lecturas y escrituras de baja latencia, con consistencia eventual entre regiones. ¿Qué solución cumple MEJOR este requisito?

A gaming company needs a NoSQL database that automatically replicates data across multiple AWS Regions with multi-active writes, so players in any Region experience low-latency reads and writes with eventual consistency across Regions. Which solution BEST meets this requirement?

A. Amazon DynamoDB con un índice secundario global (GSI)

B. Amazon ElastiCache for Redis con el modo de clúster habilitado

C. Tablas globales de Amazon DynamoDB

D. Amazon RDS Multi-AZ con réplicas de lectura entre regiones

---

63. Un arquitecto de soluciones diseña una capa de caché que debe conmutar automáticamente a un nodo réplica en segundos si el nodo principal deja de estar disponible, sin ninguna intervención de la aplicación. ¿Qué configuración de ElastiCache cumple el requisito?

A solutions architect is designing a caching layer that must automatically fail over to a replica node within seconds if the primary node becomes unavailable, without requiring any application-level intervention. Which ElastiCache configuration meets this requirement?

A. Amazon ElastiCache for Redis con el modo de clúster deshabilitado y sin nodos réplica

B. Amazon ElastiCache for Memcached con Auto Discovery habilitado en varios nodos

C. Amazon ElastiCache for Redis con Multi-AZ habilitado y al menos una réplica de lectura

D. Amazon ElastiCache for Memcached en varias zonas de disponibilidad con un solo nodo por zona

---

64. Una empresa de servicios financieros necesita una solución de recuperación ante desastres entre regiones para su base de datos Amazon Aurora MySQL, con un RPO menor de 1 segundo y un RTO menor de 1 minuto durante una caída regional. ¿Qué solución cumple MEJOR estos requisitos?

A financial services firm requires a cross-region disaster recovery solution for its Amazon Aurora MySQL database with an RPO under 1 second and an RTO under 1 minute during a regional outage. Which solution BEST meets these requirements?

A. Copias de seguridad automáticas de Aurora replicadas a una región secundaria con AWS Backup

B. AWS Database Migration Service con replicación continua a una región secundaria

C. Una implementación Multi-AZ de Amazon RDS con una réplica de lectura entre regiones

D. Amazon Aurora Global Database con una región secundaria

---

65. Un arquitecto de soluciones explica la infraestructura global de AWS a un nuevo integrante del equipo. ¿Qué afirmación describe MEJOR una zona de disponibilidad (AZ)?

A solutions architect is explaining AWS global infrastructure to a new team member. Which statement BEST describes an Availability Zone (AZ)?

A. Una agrupación lógica de buckets de Amazon S3 replicados entre países

B. Un solo rack físico de servidores dedicado a la cuenta de un cliente

C. Uno o más centros de datos independientes con energía, redes y conectividad redundantes dentro de una región de AWS

D. Un conjunto aislado geográficamente de regiones de AWS conectadas por enlaces de baja latencia

---

66. Una empresa ejecuta una aplicación de administración de contenido en instancias EC2 que deben compartir un sistema de archivos común, con los mismos archivos accesibles y escribibles a la vez desde instancias en varias zonas de disponibilidad. ¿Qué solución de almacenamiento cumple MEJOR este requisito?

A company runs a content management application on EC2 instances that must share a common file system, with the same files accessible and writable from instances in multiple Availability Zones simultaneously. Which storage solution BEST meets this requirement?

A. Volúmenes de almacén de instancias (Instance Store) replicados con un script personalizado

B. Un volumen de Amazon EBS conectado a varias instancias con Multi-Attach dentro de una zona de disponibilidad

C. Amazon EFS con destinos de montaje (mount targets) en cada zona de disponibilidad

D. Un bucket de Amazon S3 montado con un controlador FUSE personalizado

---

67. Una aplicación con una tabla global de DynamoDB multirregión permite escrituras sobre el mismo elemento, casi al mismo tiempo, en us-east-1 y eu-west-1. ¿Qué comportamiento de resolución de conflictos debe tener en cuenta el arquitecto en el diseño?

A multi-Region DynamoDB Global Table application allows writes to the same item in both us-east-1 and eu-west-1 nearly simultaneously. What conflict resolution behavior should the architect design around?

A. DynamoDB combina ambas escrituras en el elemento con un reloj vectorial y devuelve el resultado combinado

B. DynamoDB bloquea las escrituras en la tabla réplica hasta que un administrador resuelva el conflicto

C. DynamoDB rechaza la segunda escritura y devuelve una excepción ConditionalCheckFailedException al cliente

D. DynamoDB aplica que gana la última escritura según marcas de tiempo internas, y se conserva la más reciente entre las regiones

---

68. Una empresa necesita alta disponibilidad con conmutación por error en menos de un minuto Y la posibilidad de trasladar (offload) consultas de informes con mucha lectura a una instancia en espera legible, sin afectar la principal. ¿Qué implementación de RDS cumple MEJOR ambos requisitos?

A company needs both high availability with sub-minute failover AND the ability to offload read-heavy reporting queries to a readable standby without impacting the primary. Which RDS deployment BEST satisfies both requirements?

A. Una implementación de clúster de base de datos Multi-AZ de RDS con dos instancias en espera legibles

B. Una sola instancia de RDS con copias de seguridad automáticas y una copia de instantánea Multi-AZ

C. Una sola instancia de RDS con dos réplicas de lectura entre regiones

D. Una implementación clásica de instancia Multi-AZ de RDS con una instancia en espera que no se puede leer

---

69. Un arquitecto de soluciones implementó una base de datos Amazon RDS MySQL con Multi-AZ habilitado. La instancia principal deja de estar accesible por una falla de hardware subyacente. ¿Qué ocurre con la conectividad de la aplicación a la base de datos?

A solutions architect deployed an Amazon RDS MySQL database with Multi-AZ enabled. The primary database instance becomes unreachable due to an underlying hardware failure. What happens to the application's database connectivity?

A. RDS conmuta automáticamente a la instancia en espera de otra zona de disponibilidad y el punto de conexión de la base de datos no cambia

B. RDS conmuta automáticamente a una réplica de lectura y la aplicación debe actualizar su cadena de conexión

C. RDS crea una nueva instancia principal en la misma zona de disponibilidad y hay una breve interrupción hasta que se propague el DNS

D. La aplicación debe promover a mano la instancia en espera con la AWS CLI

Respuesta correcta

1. D EFA es una interfaz de red basada en ENA que agrega una interfaz de hardware que evita el sistema operativo (OS bypass). Así, las aplicaciones con MPI o NCCL se comunican con menor latencia y más estable que con la pila TCP/IP del kernel. ENA da mucho ancho de banda, pero el tráfico sigue pasando por el kernel. Una segunda ENI solo agrega otra ruta, y Global Accelerator mejora el tráfico de clientes externos, no la comunicación entre nodos del clúster.

2. B DAX es una caché en memoria administrada y compatible con DynamoDB. Solo exige un cambio pequeño en el código (cambiar el cliente) y da respuestas en microsegundos en cargas de lectura intensiva. ElastiCache for Redis obliga a la aplicación a manejar la lógica de la caché y su invalidación. Subir las RCU aumenta el rendimiento, pero no baja la latencia a microsegundos, y Global Tables sirve para replicar entre regiones.

3. C Lambda cobra solo por el tiempo de ejecución, escala sola ante picos impredecibles y no requiere administrar servidores. Es ideal para trabajos cortos (dentro de su límite de 15 minutos) a intervalos irregulares. Las instancias reservadas se pagan aunque estén inactivas, y un grupo de Auto Scaling con una instancia mínima también cuesta en reposo y exige parches y ajustes. Lightsail con tamaño fijo no escala solo y se factura de forma continua.

4. A Solo io2 Block Express admite hasta 256,000 IOPS y 4,000 MB/s por volumen con latencia de menos de un milisegundo. gp3 llega a 80,000 IOPS y 2,000 MiB/s, que no alcanza. Los límites antiguos de io2 sin Block Express eran 64,000 IOPS y 1,000 MiB/s; hoy los volúmenes io2 usan Block Express. st1 es un disco HDD para cargas secuenciales grandes, y el striping no cambia su latencia más alta.

5. B S3 Transfer Acceleration envía las cargas por la ubicación de borde más cercana y luego por la red troncal optimizada de AWS hasta el bucket. Esto mejora mucho el rendimiento de quienes están lejos. CloudFront puede acelerar solicitudes hacia un origen, pero Transfer Acceleration está hecho para cargas distribuidas a S3. La carga multiparte mejora la confiabilidad, no la ruta de red entre continentes, y la replicación copia los datos después de la carga, sin acelerarla.

6. A Las réplicas de Aurora comparten el mismo volumen de almacenamiento del clúster que la instancia principal, por eso el retraso suele ser de decenas de milisegundos, y Aurora admite hasta 15 réplicas. RDS for MySQL también admite 15 réplicas, pero usa replicación asíncrona basada en el registro binario (binlog), sin almacenamiento compartido. La instancia en espera de Multi-AZ no se puede leer: solo sirve para conmutación por error. DAX es solo para DynamoDB.

7. C io2 Block Express ofrece hasta 256,000 IOPS, latencia de menos de un milisegundo y 99.999 % de durabilidad. Está hecho para bases de datos con mucha E/S y sensibles a la latencia. gp3 llega a 80,000 IOPS aprovisionadas, que no alcanzan. st1 y sc1 son discos HDD para cargas secuenciales grandes (big data, procesamiento de registros) y tienen límites de IOPS muy por debajo de lo que necesita una base de datos transaccional.

8. D Amazon CloudFront es una red de entrega de contenido (CDN) que guarda el contenido en ubicaciones de borde distribuidas por el mundo y responde desde la más cercana, lo que reduce la latencia. ElastiCache guarda datos en memoria para el cómputo del backend, no entrega contenido al usuario final. Direct Connect es un enlace privado dedicado hacia AWS y no almacena contenido en caché. Route 53 es DNS: puede enrutar el tráfico, pero no guarda contenido en el borde.

9. D Origin Shield agrega una capa de caché adicional entre las cachés regionales de borde y el origen. Reúne las solicitudes de varias ubicaciones de borde en una sola antes de llegar al origen, así baja su carga y sube la tasa de aciertos de caché. El cifrado a nivel de campo protege datos sensibles y no influye en la caché. Las URL firmadas controlan el acceso. Los disparadores de Lambda@Edge modifican solicitudes, pero no reducen las consultas independientes al origen.

10. C Origin Shield agrega una capa de caché centralizada entre las ubicaciones de borde y el origen. Ante un fallo de caché, reúne las solicitudes de varias ubicaciones en una sola hacia el origen, y así baja su carga. Aumentar la capacidad del origen trata el síntoma y suma costo. Subir el TTL cambia la estrategia de caché, que el enunciado excluye, y puede entregar contenido vencido. Lambda@Edge ejecuta lógica en el borde, pero no reúne las consultas al origen.

11. C S3 admite al menos 3,500 solicitudes PUT/COPY/POST/DELETE y 5,500 GET/HEAD por segundo por cada prefijo particionado. Distribuir los objetos en varios prefijos aumenta el rendimiento disponible, porque permite acceso en paralelo. Son tasas base, no límites máximos fijos, y S3 escala poco a poco cuando suben las solicitudes. Transfer Acceleration acelera transferencias a larga distancia, Standard-IA cambia costo y recuperación, y el control de versiones no afecta la tasa de solicitudes.

12. B Los volúmenes io2 (e io1) admiten Multi-Attach: el mismo volumen se conecta a hasta 16 instancias basadas en Nitro dentro de una sola zona de disponibilidad, con acceso simultáneo a nivel de bloque y un sistema de archivos para clústeres. EFS da acceso compartido a archivos, no almacenamiento en bloques. S3 con Transfer Acceleration acelera cargas de objetos a larga distancia. gp3 no admite Multi-Attach.

13. A Un grupo de ubicación en clúster junta las instancias dentro de una sola zona de disponibilidad y logra red de baja latencia y alto rendimiento, ideal para HPC y MPI. El grupo disperso reparte las instancias en hardware distinto para reducir fallos correlacionados, no para bajar la latencia. El grupo por particiones limita el impacto de un fallo en sistemas como Hadoop o Cassandra. La ubicación predeterminada no garantiza cercanía ni latencia.

14. C Amazon ElastiCache es un almacén de datos en memoria administrado (Redis o Memcached) hecho para guardar en caché resultados de consultas de aplicaciones y bases de datos, y baja la latencia de lectura de milisegundos a microsegundos. DAX solo sirve para DynamoDB, no para bases relacionales como RDS. CloudFront guarda contenido en el borde para web y API. Storage Gateway conecta el almacenamiento local con AWS y no hace caché de lecturas de bases de datos.

15. C Memcached es multihilo y escala entre varios núcleos de un solo nodo, por eso va bien para guardar datos de sesión con alto rendimiento cuando no hacen falta persistencia, replicación ni estructuras de datos complejas. Redis usa un solo hilo por fragmento (shard) y ofrece durabilidad y tipos de datos avanzados, útiles si se necesita persistencia o publicación/suscripción. DAX es una caché solo para DynamoDB. RDS Proxy agrupa conexiones y no es una caché en memoria.

16. A Memcached tiene una arquitectura multihilo que escala de forma natural entre todos los núcleos de un nodo, y maximiza el rendimiento por nodo en cachés simples de clave y valor sin persistencia. Redis ejecuta los comandos en un solo hilo por fragmento; el modo de clúster habilitado escala de forma horizontal repartiendo los datos entre nodos. Redis puede usar hilos extra para la E/S, pero eso no vuelve multihilo la ejecución de comandos. Multi-AZ agrega replicación que la carga no necesita.

17. A CloudFront guarda el contenido en ubicaciones de borde de todo el mundo, así que los usuarios de Asia reciben los objetos desde una ubicación cercana y no cruzan el océano hasta us-east-1. Es una configuración simple y administrada. Transfer Acceleration acelera transferencias a larga distancia, pero no guarda objetos cerca del usuario. La replicación entre regiones complica la operación (varios buckets, sincronización). En este caso no hay instancia EC2 que ajustar.

18. C Un límite de permisos (permissions boundary) es una política administrada que fija los permisos máximos de una entidad de IAM. Los permisos efectivos son la intersección entre sus políticas basadas en identidad y el límite, así que, aunque el desarrollador adjunte una política demasiado amplia, lo que está fuera del límite se niega. Las SCP actúan a nivel de cuenta o unidad organizativa, no por rol. Las políticas de grupo no limitan lo que se adjunta directamente al rol, y las políticas de recursos controlan el acceso a cada recurso.

19. C Los roles de IAM asociados con un perfil de instancia dan credenciales temporales que se rotan solas y llegan por el servicio de metadatos de la instancia, así que no hace falta guardar credenciales de larga duración. Esto cumple el mínimo privilegio y reduce la exposición si la instancia se ve comprometida. Las claves en variables de entorno o en el código pueden filtrarse por registros, control de código o volcados de memoria, y las credenciales raíz nunca se usan en aplicaciones.

20. C AWS Shield Advanced es un nivel de pago que agrega acceso 24/7 al equipo DRT, detección y mitigación avanzadas de ataques, y créditos por los cargos de escalado causados por un ataque DDoS. Shield Standard es gratis y automático, pero solo da protección básica de red y transporte, sin DRT ni protección de costos. Las reglas basadas en tasa de WAF limitan inundaciones en la capa 7, pero no dan DRT ni créditos. GuardDuty detecta amenazas y no mitiga DDoS.

21. D Con el cifrado de EBS habilitado de forma predeterminada en la cuenta y la región, todos los volúmenes nuevos y las instantáneas que salgan de ellos se cifran solos con una clave de KMS, sin acción por volumen. El cifrado manual con herramientas de terceros agrega trabajo y el riesgo de olvidar volúmenes. Las instantáneas de EBS no están en un bucket de S3 del cliente, así que el cifrado de S3 no les afecta. Una política de denegación solo bloquearía la creación de volúmenes, no los cifraría.

22. D SSE-KMS se integra con AWS CloudTrail, que registra cada llamada a la API de KMS, como Decrypt y GenerateDataKey, junto con la entidad principal que la hizo. Así se obtiene un registro de auditoría detallado por objeto. SSE-S3 usa claves administradas por AWS y no muestra en CloudTrail el uso de cada clave. Con cifrado del lado del cliente (CMK) con clave local, AWS no puede auditar el uso de la clave. SSE-C pide la clave en cada solicitud y no genera ese registro de KMS.

23. D Los gateway endpoints de S3 solo se alcanzan desde recursos dentro de la VPC mediante rutas en la tabla de enrutamiento; no se pueden usar desde redes locales por Direct Connect o VPN. Un interface endpoint (AWS PrivateLink) crea ENI con IP privadas en la VPC que sí se alcanzan por Direct Connect, y así el acceso local a S3 es privado. Transfer Acceleration usa la internet pública, lo contrario de lo pedido. Una puerta de enlace de internet va contra el objetivo.

24. B La puerta de enlace NAT cambia la IP de origen por su IP elástica pública, así que el punto de enlace público de S3 ve esa IP y no una dirección dentro de 10.20.0.0/16; por eso se niega. Con un gateway endpoint y condiciones aws:sourceVpce o aws:SourceVpc se mantendría el alcance previsto. aws:SourceIp sí se evalúa con normalidad en tráfico de internet. CORS regula solicitudes entre orígenes en navegadores, no condiciones por IP.

25. D AWS Shield es un servicio administrado de protección contra DDoS. Standard se habilita solo y sin costo para todos los clientes, y Shield Advanced agrega detección mejorada y acceso 24/7 al equipo de respuesta a DDoS, para ataques de las capas 3/4 y 7. AWS WAF filtra solicitudes HTTP/HTTPS maliciosas (inyección SQL, XSS), pero por sí solo no es un servicio de mitigación de DDoS. Firewall Manager administra reglas de forma central, y GuardDuty detecta amenazas, no las mitiga.

26. C SSE-KMS con CloudTrail registra las llamadas a la API de KMS, como GenerateDataKey y Decrypt, e identifica quién las hizo y cuándo. Puede usar una clave administrada por AWS o por el cliente; la del cliente permite controlar la política y el ciclo de vida. Las S3 Bucket Keys reducen las llamadas a KMS, así que para auditar cada descifrado hay que dejarlas deshabilitadas. SSE-S3 no muestra el uso de cada clave. El cifrado del lado del cliente no da auditoría central, y SSE-C no registra en KMS.

27. C AWS KMS está hecho para crear, administrar y controlar claves criptográficas (CMK), con rotación y políticas de clave detalladas, y se usa en el cifrado SSE-KMS de objetos de S3. Secrets Manager guarda y rota secretos de aplicaciones, como credenciales de bases de datos, no claves de cifrado. ACM emite y administra certificados SSL/TLS para el tráfico de red. Parameter Store guarda valores de configuración como texto, pero no administra claves para cifrar datos.

28. D Conceder solo s3:GetObject y s3:PutObject sobre arn:aws:s3:::company-bucket/dev-uploads/* da únicamente las acciones necesarias y limita el ARN al prefijo exacto, que es el mínimo privilegio. AmazonS3FullAccess da acceso sin restricción a todos los buckets y acciones de la cuenta. El comodín s3:* da permisos innecesarios, como DeleteObject. Usar Resource "*" da acceso IAM a todos los buckets y objetos, un mal patrón aunque la política del bucket agregue otra capa.

29. B La evaluación de políticas de IAM sigue un orden estricto: una denegación explícita en cualquier política aplicable, sea del usuario, de un grupo o de un rol, siempre anula cualquier permiso, venga de donde venga. Las políticas del usuario no tienen prioridad sobre las del grupo, e IAM no evalúa según cuándo se adjuntó cada política. Que la denegación esté en un grupo o en el usuario no cambia el resultado: la denegación explícita manda.

30. A KMS es distinto de otros servicios: siempre hace falta una instrucción de política de clave, que es la base de confianza. Para acceso entre cuentas, la política de la CMK en la cuenta propietaria debe autorizar de forma explícita a la cuenta o entidad externa, además de la política de IAM de esa entidad; sin ella, el permiso de IAM no basta. Un comodín en Resource es un tema de buenas prácticas, no la causa. Los grants son otra forma de delegar, y las políticas de bucket no regulan acciones de KMS.

31. D En el cifrado de sobre, KMS genera una clave de datos única para cada objeto. La clave de datos en texto plano cifra el objeto localmente y luego la clave maestra (CMK) de KMS cifra esa clave de datos, que se guarda junto al texto cifrado. Así no se envían grandes cantidades de datos a KMS, que limita el tamaño de la carga, y el control de la CMK queda centralizado. Una CMK no puede cifrar directamente cargas grandes, y la clave AES propia ignora que se llama a GenerateDataKey en KMS.

32. C AWS Secrets Manager trae plantillas de rotación de Lambda ya hechas para RDS, Redshift y DocumentDB, y permite programar la rotación automática en un intervalo, como cada 30 días, con poca configuración. Parameter Store guarda valores SecureString, pero no tiene rotación nativa de credenciales de bases de datos. La rotación de KMS cambia el material de la clave cada año y no se relaciona con contraseñas. La autenticación de IAM usa tokens de corta vida y es otro mecanismo.

33. B VPC Flow Logs captura metadatos del tráfico IP hacia y desde las interfaces de red de una VPC: IP de origen y destino, puerto, protocolo y si el tráfico fue aceptado (ACCEPT) o rechazado (REJECT) según las reglas de grupos de seguridad y NACL. CloudTrail registra llamadas a la API, no el flujo de red. AWS Config sigue los cambios de configuración de recursos, no el tráfico. Amazon Inspector evalúa vulnerabilidades y exposición, no registra tráfico.

34. A AWS Network Firewall admite reglas con estado basadas en dominios (FQDN) que filtran el tráfico HTTP/HTTPS saliente por nombre de host y no por IP, lo que es clave cuando las IP del destino cambian mucho, por ejemplo detrás de una CDN o un balanceador. Los grupos de seguridad y las ACL de red solo filtran por IP/CIDR y puerto; no entienden dominios y habría que actualizarlos a mano. La política de un gateway endpoint solo controla el acceso a S3 o DynamoDB.

35. B El cifrado del almacenamiento de RDS no se puede activar en una instancia existente: es una propiedad que solo se define al crearla. La vía admitida es tomar una instantánea de la base sin cifrar, copiarla indicando una clave de KMS (así queda cifrada), restaurar una instancia nueva desde esa instantánea y hacer el cambio. Modificar o reiniciar la instancia no ofrece esa opción. Una instancia principal sin cifrar no puede tener una réplica cifrada, porque las réplicas heredan el estado de cifrado del origen.

36. B Las instancias Spot usan capacidad sobrante de EC2 y pueden dar descuentos de hasta 90 % frente a On-Demand. Son ideales para cargas flexibles y tolerantes a fallos, como el procesamiento por lotes, aunque AWS puede recuperar la capacidad con un aviso de dos minutos. Las reservadas estándar exigen un compromiso de 1 o 3 años que se paga aunque no se use. On-Demand es lo más caro por hora y no tiene descuento. Los hosts dedicados se cobran por servidor físico, por cumplimiento o licencias.

37. A Las instancias reservadas estándar a 3 años dan el mayor descuento, de hasta cerca de 72 % frente a On-Demand, para cargas estables y predecibles, porque el cliente se compromete con una configuración fija durante el plazo más largo. On-Demand no da descuento y es para cargas impredecibles. Spot es más barato, pero puede interrumpirse, y no sirve para una base de datos siempre activa. Las convertibles a 1 año permiten cambiar de familia, pero el descuento es menor.

38. A CloudFront guarda el contenido en ubicaciones de borde, así que las solicitudes repetidas se atienden sin volver a pedir los datos a S3. La transferencia de S3 a CloudFront es gratis, y la salida de CloudFront suele costar menos que la salida directa de S3 a internet, con menos costo y menos latencia. Transfer Acceleration agrega cargos y no baja el costo de las descargas. One Zone-IA reduce el costo de almacenamiento, no el de transferencia. Replicar en todas las regiones multiplica los costos.

39. C Los volúmenes gp3 incluyen en el precio base 3,000 IOPS y 125 MB/s, y el rendimiento aprovisionado es independiente del tamaño. Hoy llegan a 80,000 IOPS y 2,000 MiB/s, según los límites del volumen y la instancia. Un gp3 de 500 GB admite 16,000 IOPS y 500 MB/s a menor costo que io1 o io2, que cobran un extra por cada IOPS aprovisionada. En gp2 las IOPS dependen del tamaño (3 por GB), así que no llega a ese nivel con 500 GB sin sobredimensionar.

40. D Las instancias reservadas estándar a 3 años con pago total por adelantado dan el mayor descuento de las opciones, de hasta cerca de 72 % frente a On-Demand. Como la familia, la región y el sistema operativo no cambian, no importa que no se puedan intercambiar, y no hay razón para aceptar el descuento menor de las convertibles. Compute Savings Plans suelen tener un descuento máximo algo menor por su flexibilidad. Una reservada a 1 año sin pago inicial descuenta mucho menos.

41. A Las instancias reservadas convertibles se pueden cambiar durante el plazo por otra familia, tamaño, sistema operativo o tenencia, siempre que el valor sea igual o mayor; por eso encajan cuando se prevé migrar a generaciones nuevas. Las estándar no permiten cambiar de familia y solo admiten modificaciones limitadas, como la zona de disponibilidad. "Zonales" no es una opción de compra distinta: las reservas se limitan a una región o a una zona. Las programadas, una oferta descontinuada, eran para capacidad en horarios fijos.

42. A Los volúmenes SSD de uso general gp3 dan una base de 3,000 IOPS y 125 MiB/s sin depender del tamaño, a menor precio por GB que gp2, y permiten aprovisionar más IOPS o rendimiento por separado sin sobredimensionar el volumen. En gp2 el rendimiento base crece con el tamaño, y a menudo hay que pagar más capacidad solo para tener IOPS. io2 Block Express es para cargas críticas con muchas IOPS y cuesta más. st1 es HDD para cargas secuenciales grandes, no de uso general.

43. D Las instancias Spot dan descuentos de hasta 90 % frente a On-Demand y son ideales para trabajos por lotes tolerantes a interrupciones, como una transcodificación que guarda su progreso y se reanuda. Las reservadas exigen un compromiso de 1 o 3 años que no encaja con una carga que corre poco cada noche. On-Demand es lo más caro por hora. Los hosts dedicados se usan por cumplimiento o licencias, no para ahorrar, y son la opción más cara.

44. D Las instancias reservadas de RDS dan descuentos de hasta 69 % frente a On-Demand a cambio de un compromiso de 1 o 3 años, lo que encaja con una base de datos estable y predecible. On-Demand no da descuento por uso continuo. RDS no tiene modelo Spot: esa opción es solo de EC2. Aurora Serverless v2 fijo en su capacidad máxima pierde la ventaja del escalado automático y suele costar más que una instancia reservada del tamaño adecuado.

45. B S3 Glacier Flexible Retrieval ofrece recuperación acelerada en 1 a 5 minutos y cuesta mucho menos que Standard-IA para datos de archivo poco consultados, así que cumple "una vez al año, en minutos" al menor costo. Deep Archive es más barato por GB, pero su recuperación estándar tarda unas 12 horas, y no cumple lo de minutos. Standard-IA y One Zone-IA son para acceso mensual, no anual, y con este patrón cuestan más por GB que las clases Glacier.

46. B Con S3 Requester Pays, quien descarga los objetos paga la transferencia de datos y las solicitudes, y no el propietario del bucket; está pensado justo para conjuntos de datos públicos o compartidos con terceros. Object Lock impone retención de tipo escribir una vez y leer muchas (WORM) para cumplimiento y no traslada costos. Con Transfer Acceleration el propietario sigue pagando, y además hay un recargo. La replicación en la misma región copia datos y no cambia quién paga las descargas.

47. B S3 Intelligent-Tiering vigila los patrones de acceso a nivel de objeto y los mueve solo entre los niveles de acceso frecuente, poco frecuente y de archivo, sin cargos de recuperación y con poca carga operativa. Es ideal cuando el acceso es impredecible. Las reglas de ciclo de vida hacia Standard-IA o Glacier exigen adivinar cuándo se usarán; las lecturas posteriores tienen costo, y borrar antes de la duración mínima también. One Zone-IA pierde la resiliencia entre zonas. El ahorro puede superar el pequeño cargo mensual de monitoreo.

48. B Con las reservadas de pago total por adelantado se paga todo el costo al inicio del plazo, y a cambio AWS da el mayor descuento frente a On-Demand para ese plazo, porque recibe el pago completo de inmediato. El pago inicial parcial pide menos al inicio, se factura el resto por hora y da un descuento algo menor. Sin pago inicial no se paga nada al comienzo y es el descuento más bajo de los tres. Los pagos mensuales sin compromiso no son una opción de reservadas, sino una facturación tipo On-Demand.

49. A Con las instancias On-Demand se paga la capacidad de cómputo por segundo en Linux, o por hora, sin pago inicial ni contrato a largo plazo. Dan la mayor flexibilidad para cargas con picos, impredecibles o de corta duración, como pruebas de desarrollo. Las instancias reservadas y los Savings Plans exigen un compromiso de 1 o 3 años a cambio de un descuento, y no sirven para necesidades cortas e impredecibles. Spot también tiene poco compromiso, pero se puede interrumpir con dos minutos de aviso, y On-Demand no.

50. A La replicación entre regiones copia objetos de un bucket a otro en otra región y cobra la transferencia entre regiones por cada GB replicado. Ese cargo no existe en la replicación en la misma región, porque el tráfico no sale de la región. Los cargos de solicitudes PUT y de almacenamiento en el destino se aplican en ambas, porque las dos escriben y guardan réplicas. Replication Time Control es un complemento opcional para las dos, así que no las distingue.

51. D S3 Intelligent-Tiering vigila los patrones de acceso y mueve los objetos entre sus niveles de acceso inmediato sin afectar el rendimiento ni cobrar recuperación; es ideal cuando el acceso es desconocido o cambia. Sus niveles opcionales Archive Access y Deep Archive Access exigen restaurar antes de acceder. S3 Standard-IA exige saber de antemano que el acceso es poco frecuente y cobra recuperación. One Zone-IA usa una sola zona y no cambia de nivel solo. Glacier Instant Retrieval es un nivel de archivo fijo.

52. C Una instancia NAT en una instancia EC2 pequeña solo genera el costo normal de EC2 más la transferencia de datos, y suele salir más barata en entornos de desarrollo con poco tráfico y sin criticidad que una puerta de enlace NAT, con su cargo por hora y por GB procesado. Las puertas de enlace NAT, sobre todo una por zona o dos para alta disponibilidad, son administradas y muy disponibles, pero cuestan más y son para producción. Direct Connect es una conexión dedicada con la red local, mucho más cara.

53. B Amazon EventBridge es un bus de eventos sin servidor hecho para enrutar eventos de varias fuentes a varios destinos con reglas de filtrado por contenido, ideal para arquitecturas de microservicios con distribución (fan-out). SQS es una cola punto a punto, sin filtrado nativo por contenido hacia muchos destinos. Step Functions orquesta flujos de trabajo, no enruta eventos independientes. Kinesis Data Streams sirve para análisis de flujos de alto volumen, no para enrutar por reglas.

54. B AWS Global Accelerator usa la red global de AWS y direcciones IP estáticas anycast para dirigir tráfico TCP/UDP al mejor punto de conexión saludable entre regiones, según latencia y estado. Es ideal para cargas sensibles a la latencia que no son HTTP, como los juegos multijugador. CloudFront está optimizado para caché HTTP/HTTPS. El enrutamiento por latencia de Route 53 actúa en la capa DNS y reacciona más lento al estado del punto de conexión. El balanceo entre zonas actúa dentro de un balanceador, no entre regiones.

55. A En la conmutación por error de RDS Multi-AZ cambia el registro DNS del punto de conexión fijo de la instancia para apuntar a la instancia en espera, que pasa a ser la principal en otra zona. La aplicación solo se reconecta cuando el DNS se propaga, sin cambiar código ni configuración. Las comprobaciones de Route 53 no forman parte de ese mecanismo. Las réplicas de lectura son copias asíncronas aparte y no se promueven solas: solo se promueve la instancia en espera síncrona.

56. B Las tablas globales de DynamoDB son una base de datos multirregión y multiactiva totalmente administrada, con replicación automática y asíncrona y resolución de conflictos de tipo "gana la última escritura". Dan lecturas y escrituras de baja latencia en cada región participante. RDS Multi-AZ da alta disponibilidad solo dentro de una región. Las réplicas de lectura de RDS solo escriben en una región y hay que promoverlas a mano para escribir. ElastiCache for Redis es una caché dentro de una región, no almacenamiento durable multirregión.

57. D Backup and restore es la estrategia de recuperación más barata: guarda copias (por ejemplo, en Amazon S3 o con AWS Backup) y reconstruye la infraestructura solo cuando ocurre el desastre. Recuperar en 24 horas y hacer copias periódicas (por ejemplo, diarias) cumple sin problema un RTO y un RPO de 24 horas con un costo continuo mínimo. Pilot light, warm standby y multisitio mantienen infraestructura en ejecución, total o parcial, en una segunda región, con costos de cómputo o replicación que aquí no hacen falta.

58. B Warm standby mantiene en una región secundaria una réplica reducida y totalmente funcional del entorno de producción; en un desastre se escala para atender toda la carga. Tiene un RTO más rápido que pilot light, con mayor costo continuo. Pilot light mantiene en ejecución solo lo esencial, como bases de datos replicadas, y el resto debe iniciarse o aprovisionarse. Backup and restore tiene el mayor RTO y RPO, porque los recursos se crean tras declarar el desastre. Multisitio sirve tráfico desde varias regiones a la vez.

59. B RDS Multi-AZ replica los datos de forma síncrona en una instancia en espera de otra zona y conmuta solo (normalmente en 60 a 120 segundos) si falla la zona principal, lo que cumple el requisito de disponibilidad. Las instantáneas diarias solo protegen contra la pérdida de datos, no contra la caída de una zona, y restaurar tarda. Una réplica de lectura en la misma zona no da redundancia entre zonas. Un ELB equilibra el tráfico de la aplicación, no la conmutación de la base de datos, que seguiría siendo un punto único de falla.

60. A Las tablas globales de DynamoDB resuelven las escrituras simultáneas del mismo elemento con la regla de que gana la última escritura, según marcas de tiempo internas, sin intervención de la aplicación. ConditionalCheckFailedException solo ocurre cuando la aplicación usa escrituras condicionales, no por conflictos normales de replicación entre regiones. DynamoDB no usa relojes vectoriales ni combina atributos. No existe un mecanismo que pause la replicación para resolver a mano con Lambda.

61. B Warm standby mantiene en la región de recuperación una réplica reducida y funcional de cada capa de la aplicación, que se escala a toda la carga en minutos. Cumple un RTO de 10 minutos y un RPO bajo, sin pagar siempre la capacidad completa duplicada. Backup and restore suele dar un RTO de horas. Pilot light solo mantiene los servicios de datos (a menudo solo la base de datos), y el cómputo debe aprovisionarse en el evento, lo que suele pasar de 10 minutos. Multisitio cumpliría, pero su costo lo excluye la restricción.

62. C Las tablas globales de DynamoDB dan replicación multirregión y multiactiva totalmente administrada: la aplicación de cada región lee y escribe en local y los cambios se propagan a las demás. Un índice secundario global solo agrega otros patrones de consulta dentro de una tabla y región. RDS Multi-AZ con réplicas entre regiones solo tiene una región principal con escritura. ElastiCache for Redis escala dentro de una región y no replica entre regiones de forma multiactiva.

63. C ElastiCache for Redis con Multi-AZ y al menos una réplica de lectura admite conmutación automática: detecta la falla del nodo principal, promueve una réplica y actualiza el DNS del punto de conexión principal, sin reconfigurar la aplicación. Los clientes deben reconectar y reintentar, y el tiempo real varía. Memcached no promueve réplicas; Auto Discovery solo ayuda a ubicar nodos. Redis sin réplicas no tiene a quién promover, y sin réplica no se puede habilitar la conmutación automática de Multi-AZ.

64. D Aurora Global Database con una región secundaria usa replicación dedicada a nivel de almacenamiento, con un retraso típico menor de un segundo, y se recupera de una caída regional promoviendo la región secundaria, normalmente en menos de un minuto. Son valores típicos, no límites garantizados. Una réplica de RDS entre regiones usa replicación asíncrona del motor, con retraso de segundos o minutos, y exige promoción. DMS agrega complejidad y no tiene esas capacidades. Restaurar copias replicadas tarda mucho más.

65. C Una zona de disponibilidad son uno o más centros de datos independientes, con energía, redes y conectividad redundantes, en instalaciones separadas y aisladas de las fallas de otras zonas de la misma región. Las regiones contienen varias zonas, y no al revés, así que "conjunto de regiones" es incorrecto. Un rack es una unidad demasiado pequeña, y los buckets de S3 son un servicio de almacenamiento. Esta jerarquía (región > zona > centro de datos) es la base de todo diseño Multi-AZ.

66. C Amazon EFS con destinos de montaje en cada zona es un sistema de archivos NFS elástico y totalmente administrado, con lectura y escritura simultáneas desde miles de instancias EC2 de varias zonas; es ideal para cargas compartidas multi-AZ. EBS Multi-Attach se limita a una zona, a volúmenes io1/io2 y a sistemas de archivos para clústeres. S3 es almacenamiento de objetos, no un sistema de archivos POSIX compartido. El Instance Store es efímero, local a una instancia y se pierde al detenerla o terminarla.

67. D En las tablas globales con consistencia eventual multirregión, DynamoDB aplica que gana la última escritura según marcas de tiempo internas, así que escrituras simultáneas del mismo elemento en regiones distintas pueden sobrescribirse sin aviso. Asignar a cada región su propia propiedad de escritura evita estos conflictos; las escrituras condicionales se evalúan en la réplica local y no dan control de concurrencia entre regiones. DynamoDB no rechaza con excepción, no usa relojes vectoriales ni exige resolución manual.

68. A La implementación más nueva de clúster de base de datos Multi-AZ de RDS (para MySQL y PostgreSQL) tiene dos instancias en espera legibles con replicación semisíncrona y una conmutación automática que suele completarse en menos de 35 segundos, así las consultas de informes no tocan la principal. La instancia en espera de un Multi-AZ clásico no es legible. Las réplicas de lectura son asíncronas, con más retraso y sin esa conmutación rápida. Las instantáneas son una herramienta de recuperación, no de alta disponibilidad.

69. A RDS Multi-AZ replica los datos de forma síncrona en una instancia en espera de otra zona. Si falla la principal, RDS inicia solo la conmutación y cambia el registro DNS (CNAME) para apuntar a la instancia en espera, normalmente en 60 a 120 segundos y sin cambiar el punto de conexión. La conmutación a una réplica de lectura es incorrecta, porque las réplicas son asíncronas y no forman parte de Multi-AZ. Recrear en la misma zona no es la conmutación, y la promoción manual no hace falta.

Palabras clave en inglés

Availability Zone (AZ)	zona de disponibilidad	Uno o más centros de datos aislados dentro de una región.
cost-effective	rentable	Que cumple lo que se pide con el menor gasto posible.

high availability	alta disponibilidad	Diseño que mantiene el servicio en línea con interrupciones mínimas.
fault tolerance	tolerancia a fallas	Capacidad de seguir operando aunque falle un componente.
failover	conmutación por error	Cambio a un recurso de respaldo cuando falla el principal.
recovery time objective (RTO)	objetivo de tiempo de recuperación	Tiempo máximo aceptable para restaurar el servicio tras una falla.
recovery point objective (RPO)	objetivo de punto de recuperación	Cantidad máxima de datos recientes, medida en tiempo, que aceptas perder.
load balancer	balanceador de carga	Reparte el tráfico entre varios servidores o destinos.
target group	grupo de destino	Conjunto de destinos a los que el balanceador envía solicitudes.
health check	comprobación de estado	Prueba periódica que confirma si un destino responde bien.
threshold	umbral	Valor límite que provoca un cambio de estado o una acción.
Auto Scaling group	grupo de Auto Scaling	Conjunto de instancias que aumenta o disminuye según reglas o demanda.
decoupling	desacoplamiento	Separar componentes para que la falla de uno no detenga a otros.
message queue	cola de mensajes	Guarda mensajes hasta que otro componente pueda procesarlos.
least privilege	mínimo privilegio	Dar solo los permisos necesarios para una tarea.
IAM role	rol de IAM	Identidad con permisos que se asume de forma temporal.
IAM policy	política de IAM	Documento que permite o niega acciones sobre recursos.
trust policy	política de confianza	Define quién puede asumir un rol.
cross-account access	acceso entre cuentas	Permiso para usar recursos de otra cuenta de AWS.
confused deputy problem	problema del suplente confuso	Alguien sin permisos logra que una entidad con permisos actúe por él.
multi-factor authentication (MFA)	autenticación multifactor	Pide una segunda prueba de identidad además de la contraseña.
encryption at rest	cifrado en reposo	Protege los datos mientras están almacenados.
encryption in transit	cifrado en tránsito	Protege los datos mientras viajan por la red.

secrets management	administración de secretos	Guardar y rotar contraseñas y claves sin escribirlas en el código.
virtual private cloud (VPC)	nube privada virtual	Red aislada dentro de AWS que tú configuras.
subnet	subred	Rango de direcciones IP dentro de una VPC.
security group	grupo de seguridad	Firewall virtual que controla el tráfico de un recurso.
VPC endpoint	punto de enlace de VPC	Conexión privada a servicios de AWS sin pasar por internet.
storage class	clase de almacenamiento	Categoría de S3 según frecuencia de acceso, costo y disponibilidad.
infrequent access (IA)	acceso poco frecuente	Almacenamiento para datos que se leen pocas veces.
lifecycle policy	política de ciclo de vida	Regla que mueve o borra objetos después de cierto tiempo.
access pattern	patrón de acceso	Cómo y con qué frecuencia se leen o escriben los datos.
latency	latencia	Tiempo que tarda en llegar una respuesta.
throughput	rendimiento, tasa de transferencia	Cantidad de datos o trabajo procesado por unidad de tiempo.
caching	almacenamiento en caché	Guardar copias temporales para responder más rápido.
Spot Instance	instancia Spot	Capacidad sobrante más barata que AWS puede interrumpir.
Reserved Instance	instancia reservada	Descuento a cambio de un compromiso de uno a tres años.
Dedicated Host	host dedicado	Servidor físico exclusivo, útil para licencias y cumplimiento.
right-sizing	ajuste del tamaño de los recursos	Elegir recursos del tamaño que la carga realmente necesita.
operational overhead	carga operativa	Trabajo de administración y mantenimiento que exige una solución.
Elastic Fabric Adapter (EFA)	interfaz de red EFA	Interfaz de red que evita el kernel para comunicación HPC de baja latencia.
Origin Shield	capa de caché ante el origen	Caché central de CloudFront que reduce las solicitudes al origen.
permissions boundary	límite de permisos	Máximo de permisos que puede tener un rol o usuario de IAM.
warm standby	espera semiactiva	Copia reducida pero funcional del entorno, lista para escalar tras un desastre.

pilot light	luz piloto	Estrategia de recuperación que solo mantiene activos los servicios centrales, como la base de datos.

Examundo es independiente. No está afiliado con los organismos que hacen estos exámenes ni tiene su aprobación. Las preguntas son originales, no son del examen real. examundo.tech/es/aws-solutions-architect/